WHAT IS CLAIMED IS:

1. A decryption device, comprising:

an internal-key storage section for storing an internal-key;

a content-key storage section for storing a content-key;

a determination section for determining whether or not a value of the content-key storage section in its initial state and a current value of the content-key storage section are different; and

an operation section, the operation section including

a first decrypting section which, when an encrypted content-key is input to the operation section, decrypts the encrypted content-key using the internal-key so as to obtain a content-key and stores the content-key in the content-key storage section, and

a second decrypting section which, when an encrypted content is input to the operation section and the determination section determines that the value of the content-key storage section in its initial state and the current value of the content-key storage section are different, decrypts the encrypted content using the current value of the content-key storage section as a content-key so as to obtain a first output data and outputs the first output data to outside of the decryption device.

2. A decryption device according to claim 1, further comprising a content-key generation section which generates a content-key for encrypting a content based on random numbers and stores the generated content-key in the content-key storage section, wherein the operation section

further includes

a first encrypting section which encrypts the content-key for encrypting a content so as to obtain an encrypted content-key and outputs the encrypted content-key to outside of the decryption device, and

a second encrypting section which, when a content is input to the operation section and the determination section determines that the value of the content-key storage section in its initial state and the current value of the content-key storage section are different, encrypts the content using the current value of the content-key storage section as a content-key so as to obtain a second output data and outputs the second output data to outside of the decryption device.

3. A decryption device according to claim 1, further comprising a mutual authentication section for determining whether or not a mutual authentication has been made between the mutual authentication section and a storage device which is located outside the decryption device and stores the encrypted content-key,

wherein the second decrypting section decrypts the encrypted content when the mutual authentication section determines that the mutual authentication has been made.

4. A decryption device according to claim 1, wherein:

the internal-key storage section stores a plurality of internal-keys; and

the internal-key storage section selects one of the plurality of internal-keys as the internal-key based on internal-key selection information input from outside the decryption device to the decryption device.